

(1) Verify the digital signature as provided in FIPS 186-3, as incorporated by reference in § 1311.08.

(2) Check the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.

(3) Archive the digitally signed record. The pharmacy record must retain an indication that the prescription was verified upon receipt. No additional digital signature is required.

#### § 1311.215 Internal audit trail.

(a) The pharmacy application provider must establish and implement a list of auditable events. The auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.

(2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the pharmacy application.

(4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The pharmacy application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) The pharmacy must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescrip-

tion records. Any such incidents must be reported to the pharmacy application service provider, if applicable, and the Administration within one business day.

#### § 1311.300 Application provider requirements—Third-party audits or certifications.

(a) Except as provided in paragraph (e) of this section, the application provider of an electronic prescription application or a pharmacy application must have a third-party audit of the application that determines that the application meets the requirements of this part at each of the following times:

(1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions.

(2) Whenever a functionality related to controlled substance prescription requirements is altered or every two years, whichever occurs first.

(b) The third-party audit must be conducted by one of the following:

(1) A person qualified to conduct a SysTrust, WebTrust, or SAS 70 audit.

(2) A Certified Information System Auditor who performs compliance audits as a regular ongoing business activity.

(c) An audit for installed applications must address processing integrity and determine that the application meets the requirements of this part.

(d) An audit for application service providers must address processing integrity and physical security and determine that the application meets the requirements of this part.

(e) If a certifying organization whose certification process has been approved by DEA verifies and certifies that an electronic prescription or pharmacy application meets the requirements of this part, certification by that organization may be used as an alternative to the audit requirements of paragraphs (b) through (d) of this section, provided that the certification that determines that the application meets the requirements of this part occurs at each of the following times:

(1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions.